REMARKS

I. Claim Rejections - 35 US §112

The Examiner rejected claims 37, 39, 44, 47 and 52 under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. The Examiner argued that the claims contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor, at the time the application was filed, had possession of the claimed invention.

Regarding claim 37, the Examiner argued that support has not been pointed out by the Applicant, nor could support be easily found in the specification, for the new limitation that a single device contains both a fob and a badge.

The Applicant notes that claim 37 has been cancelled with this amendment in response to this rejection, rendering moot the Examiner's argument.

Regarding claims 39 and 47, the Examiner argued that support has not been pointed out by the Applicant, nor could support be easily found in the specification, for the new limitation of authorizing access to information.

The Applicant respectfully disagrees with this assessment and notes that in response to this rejection, claims 39 and 47 have been amended to change "information" to "a controlled apparatus or process". This limitation is disclosed in the Applicant's paragraph [0001]. The Applicant invites the Examiner to review paragraph [0001] of Applicant's specification.

Regarding claims 44 and 52, the Examiner argued that support has not been pointed out by the Applicant, nor could support be easily found in the specification, for the new limitation of a card reader.

The Applicant respectfully disagrees with this assessment and notes that in response to this rejection, claims 44 and 52 have been amended to change the term "card" to "magnetic stripe". This limitation is disclosed in the Applicant's

paragraph [0017]. It is believed that the amendments to claims 44 and 52 now overcomes the Examiner's rejection under 35 U.S.C. §112 with respect to claims 44 and 52.

The Examiner rejected claim 25 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicant regards as the invention.

Regarding claim 25, the Examiner argued that claim 25 depends upon cancelled claim 17. The Examiner stated that for consideration of art rejections below, it is considered that claim 25 depends upon claim 14.

The Applicant notes that claim 25 has been amended in response to this rejection to make the claim dependent upon claim 14. The Examiner's argument with respect to claim 17 is therefore rendered moot because claim 25 properly depends from claim 14.

Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §112 rejections of claims 39, 44, 47 and 52 be withdrawn.

II. Claim Rejections - 35 USC § 102

Requirements for Prima Facie Anticipation

A general definition of *prima facie* unpatentability is provided at 37 C.F.R. §1.56(b)(2)(ii):

> A *prima facie* case of unpatentability is established when the information *compels a conclusion* that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability. (*emphasis added*)

"Anticipation requires the disclosure in a single prior art reference of each element of the claim under consideration." *W.L. Gore & Associates v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303, 313 (Fed. Cir. 1983) (citing *Soundscriber Corp. v.*

United States, 360 F.2d 954, 960, 148 USPQ 298, 301 (Ct. Cl.), *adopted*, 149 USPQ 640 (Ct. Cl. 1966)), *cert. denied*, 469 U.S. 851 (1984). Thus, to anticipate the applicants' claims, the reference cited by the Examiner must disclose each element recited therein. "There must be no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention." *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565, 18 USPQ 2d 1001, 1010 (Fed. Cir. 1991).

To overcome the anticipation rejection, the applicants need only demonstrate that not all elements of a *prima facie* case of anticipation have been met, *i.e.*, show that the reference cited by the Examiner fails to disclose every element in each of the applicants' claims. "If the examination at the initial state does not produce a prima face case of unpatentability, then without more the applicant is entitled to grant of the patent." *In re Oetiker*, 977 F.2d 1443, 24 USPQ 2d 1443, 1444 (Fed. Cir. 1992).

Requirements for Inherency-Based Anticipation

There are a number of factors that must be considered when attempting to establish inherency as a basis for anticipation. Inherency should only be applied under very limited circumstances. That is, inherency permits in very limited circumstances, an invention to be anticipated by prior art that is lacking minor, well-known features in the claimed invention. If the "missing subject matter" is "inherent" or necessarily disclosed in the prior art reference, then anticipation can exist. As stated by the Federal Circuit (see In re Sun USPQ2d 1451, 1453 (Fed. Cir. 1983)

> …To serve as an anticipation when the reference is silent about the asserted inherent characteristic, such gap in the reference may be filled with recourse to intrinsic evidence. Such evidence must make clear that the missing descriptive matter is necessarily present in the thing described in the reference and that it would be so recognized by persons of ordinary skill.

In this regard, the CCPA has added that "'[i]nherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may

result from a given set of circumstances is not sufficient". See In re Oelrich, 666 F.2d 578, 581, 212 USPQ 323, 326 (C.C.P.A. 1981) (quoting Hansgrig v. Kemmer, 102 F.2d 212, 214, 40 USPQ 665, 667 (C.C.P.A. 1930). That is, the missing element or function must necessarily result from the prior art reference.

Additionally, when an Examiner's rejection relies on inherency, it is incumbent upon the Examiner to point to the page and line of the prior art that justifies the rejection based on an inherency theory. The Examiner must not leave the Applicant to guess at the basis of the inherency rejection.

The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (reversed rejection because inherency was based on what would result due to optimization of conditions, not what was necessarily present in the prior art); *In re Oelrich*, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.' " *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (citations omitted).

"In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art." *Ex parte Levy,* 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis in original).

Berardi

The Examiner rejected claims 26-34 under 35 U.S.C. §102(e) as being anticipated by Berardi et al. (U.S. Patent Application No. 2003/0167207), hereinafter referred to as "Berardi".

The Examiner argued that Berardi shows a method for providing access to a financial transaction, where the system includes two versions of the transponder 102. The Examiner admitted that the first embodiment of transponder 102 does not include a fingerprint reader (citing FIG. 2); the Examiner interpreted this as a badge. The Examiner stated that the second embodiment of transponder 102 includes a fingerprint reader (citing FIG. 9); this is interpreted by the Examiner s a keyfob.

The Examiner argued that the FIG. 9 transponder sends the fob ID (citing stored in memory 214) with the fingerprint so both can be authenticated. The Examiner stated that when the data is read from the transponder, a comparison is made to authorize financial access, arguing that this meets the limitation of determining if the received code is authentic and providing access upon authentication.

The Examiner argued that if the data is from a badge, the authorization step compares account data (or the transponder ID) (citing paragraph [0059]), and if the data is from a keyfob, the authorization step compares the fingerprint data (citing paragraph 141). It is the Examiner's position that in order to compare the received data from the FIG. 9 transponder with stored fingerprint data, a decision inherently is made that the data received includes fingerprint data. The Examiner stated that this meets the limitation of determining if the code is from a badge or keyfob.

The Applicant respectfully disagrees with this assessment and notes that independent claim 26 has been amended to include the claim limitations of:

1. transmitting an RF signal containing an authentication code from either a first type of access device or a second type of access device;

and 2. wherein the first type of authentication code is transmitted from the first type of access device and the second type of authentication code is transmitted from the second type of access device.

The Applicant submits that support for such amendments is provided by Applicant's specification. The Applicant further notes that independent claim 32 has been amended to include the limitation of: wherein the authentication code from the badge is retrieved from a memory location contained within the badge. Support for the amendment to claim 32 is also adequately provided by Applicant's specification in paragraphs [0018] - [0019] as follows:

> [0018] As shown in FIG. 2, the chip 22 includes a transceiver 28, a memory 30, and a power supply 32, and is coupled to an antenna 34 of the badge 20. Specifically, the transceiver 28 is coupled to the antenna 34 and the memory 30. The memory 30 stores an identifier that uniquely identifies a person to whom the badge 20 is issued. This identifier may comprise one or more symbols such as, for example, numbers and/or letters. The power supply 32 powers the transceiver 28 and the memory 30.
>
> [0019] The transceiver 16 of the reader 12 transmits the RF stimulus signal to the badge 20. In response to the RF stimulus signal, the transceiver 28 reads the identifier from the memory 30, and transmits the stored identifier as an authentication code in an RF signal through the antennas 34 and 18 to the transceiver 16.

The Applicant's invention is an access system and method wherein the reader is capable of interrogating and receiving data from both a badge and a fingerprint keyfob. The primary component of the invention is this *dual technology reader*; i.e. the *reader* can transmit an interrogation signal and receive signals from two types of access authentication devices. This feature is claimed in claim 26 as a first type and second type of authentication code and in claim 32 as analyzing at least one RF signal containing an authentication code to determine whether the authentication code is derived from a keyfob or from a badge. The Applicant discloses a *reader* that is capable of reading the single authorization code form a badge or the dual authorization code of a digitalized fingerprint combined with a rolling code or a

keyfob authorization code. This is accomplished with a single reader. This is the Applicant's invention of a *dual technology* authentication system.

This is disclosed in the Applicant's paragraphs [0025] - [0026] as follows:

> [0025] The processor 14 of the reader 12 executes a program 60 which is shown by way of a flow chart in FIG. 4. As shown in FIG. 4, the badge 20 transmits a badge authentication code in an RF signal. *The processor 14 at a block 62 reads the badge authentication code and determines at a block 64 whether the badge authentication code has been received from the badge 20.* Assuming that the badge authentication code has been received from the badge 20, the processor 14 at a block 66 authenticates the badge authentication code by comparing the identifier of the badge authentication code to a list of authentic identifiers, and determines at a block 68 if the identifier of the badge authentication code received from the badge 20 matches one of the authentic identifiers in the list of authentic identifiers. If the processor 14 determines at the block 68 that the identifier of the badge authentication code received from the badge 20 matches one of the authentic identifiers in the list of authentic identifiers, the processor 14 at a block 70 grants access to a restricted area or apparatus or otherwise permits a person to perform a function or process such as operate a computer. On the other hand, if the processor 14 determines at the block 68 that the identifier of the badge authentication code received from the badge 20 does not match one of the authentic identifiers in the list of authentic identifiers, the processor 14 at a block 72 denies access to a restricted area or apparatus or otherwise prevents a person from performing a function or process.
>
> [0026] Additionally or alternatively, the keyfob 24 may transmit a keyfob authentication code in an RF signal. *The processor 14 at the block 62 reads the keyfob authentication code and determines at the block 64 whether the keyfob authentication code has been received from the keyfob 24*. If the keyfob authentication code has been received from the keyfob 24, the processor 14 at a block 74 authenticates the keyfob authentication code by comparing the digitized fingerprint signature of the keyfob authentication code to a list of authentic digitized fingerprint signatures, and by comparing the rolling identifier of the keyfob authentication code to a rolling identifier synchronously maintained by the processor 14. The processor 14 determines at the block 68 if the digitized fingerprint signature of the keyfob authentication code matches one of the digitized fingerprint signatures from the list of authentic digitized fingerprint signatures and if the rolling identifier of the keyfob authentication code matches the rolling identifier that is maintained by the processor 14. If the processor 14 determines at the block 68 that the digitized fingerprint signature of the keyfob authentication code matches one of the digitized fingerprint signatures from the list of authentic digitized fingerprint signatures and also determines that the rolling identifier of the keyfob authentication code matches the rolling identifier that it maintains, the processor 14 at the block 70 grants access to a restricted area or apparatus or otherwise permits a person to perform a function or process. On the other hand, if the processor 14 determines at the block 68 that the digitized fingerprint signature

> of the keyfob authentication code does not match one of the digitized fingerprint signatures from the list of authentic digitized fingerprint signatures and/or that the rolling identifier of the keyfob authentication code does not match the rolling identifier that is maintained by the processor 14, the processor 14 at the block 72 denies access to a restricted area or apparatus or otherwise prevents a person performing a function or process. (emphasis added)

Berardi does not disclose this limitation of a dual technology reader. This "dual" aspect is not taught, disclosed or suggested by Berardi. The Examiner cites Berardi for disclosing both a badge (RFID transponder with an authorization code) and a fingerprint keyfob (RFID transponder with a biometric sensor); however, Berardi does not disclose a *reader* which can receive signals from both a badge AND a keyfob. Berardi does disclose "an alternate embodiment" when the biometric sensor RFID transponder is disclosed. Berardi paragraph [0140] shows that this is an alternate embodiment; i.e. the biometric sensor can be used only as an alternative embodiment to a system which does not include biometric data. In other words, the reader of Berardi could either read data from a badge or data from a keyfob, but not BOTH. Berardi does not disclose at any point that the reader 104 is capable of sending an interrogation signal to both a badge and a keyfob and then receiving the respective authentication codes from both the badge and keyfob.

The Examiner has argued that a decision is inherently made that the data received includes fingerprint data, but Berardi has disclosed a reader capable of reading a transponder with fingerprint data only as an alternate embodiment. In the alternate embodiment system, no decision is made as to whether the data is from a badge or a keyfob as it can *only* read fingerprint keyfob data. The reader of Berardi can alternatively either read data from a badge or a keyfob, but not both.

If the reader, in the alternative embodiment, can *only* receive fingerprint data, then no decision is inherently made that the data includes fingerprint data, as *all* of the received data *must* include fingerprint data. In the aforementioned requirements for inherency-based anticipation, it is stated by the Federal Circuit that the missing element or function *must* necessarily result from the prior art

reference. Berardi has not disclosed that a decision is inherently made that the data received includes fingerprint data. The Examiner has not cited any specific location in Berardi where the reader can receive data form both a badge device and a fingerprint keyfob device. The Applicant respectfully requests that the Examine provide a specific citation in Berardi for a reader which is capable of reading both a badge and a fingerprint keyfob at the same time. Without a specific citation in Berardi, a *prima facie* case of anticipation has not been made and the Applicant is entitled to a grant of the patent as Berardi does not disclose each and every limitation of the Applicant's independent claims.

From an inherency-based anticipation standpoint, it is also clear that Berardi does not inherently anticipate Applicant's claim limitations, because in relying upon the theory of inherency, the Examiner has not provided a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly "inherent" characteristic of a decision made that the data received includes fingerprint data necessarily flows from the disclosure of the Berardi reference.

Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §102(e) rejections of claims 26-34, based on the Berardi reference, be withdrawn.

Fitzgibbon

The Examiner rejected claims 38-41, 45-49 and 53 under 35 U.S.C. §102(e) as being anticipated by Fitzgibbon et al. (U.S. Patent Application No. 2003/0210131), hereinafter referred to as "Fitzgibbon".

The Examiner argued that Fitzgibbon teaches an access security system where a transponder can send codes to a garage door for access authorization. The Examiner argued that the portable transmitter (citing authorization module) can additionally include a fingerprint reader to send information regarding the user's fingerprint, also for authorization. The Examiner argued that Fitzgibbon includes a processor (citing FIG. 4) in communication with the transmitters to process data

received and make an authorization determination (citing FIG. 8). The Examiner stated that a gate lock is considered a door lock.

The Examiner has argued that Fitzgibbon teaches that in this type of system the use of rolling codes can improve the security of the system (citing FIG. 5). The Examiner stated that Fitzgibbon incorporates by reference U.S. Patent No. 5,949,349 and stated that the system disclosed can be used to open the gates as described in U.S. Patent No. 5,949,349. The Examiner states that this patent discusses a plurality of authorization modules associated with a gate to allow entry into the facility (citing abstract of U.S. Patent No. 5,949,349). The Examiner argued that, therefore, using Fitzgibbon's authorization in a plural transmitter gate or garage door opening system is taught and shown by Fitzgibbon. The Examiner argued that Fitzgibbon discusses learning a rolling code and storing in an associated table via an address of the table, looking up in the code table is considered a shared and indexed mathematical function as claimed (citing Fitzgibbon paragraph [0052]).

The Applicant respectfully disagrees with this assessment and notes that independent claim 38 has been amended as follows:

> An access control system, comprising:
> an access device; and
> a plurality of authorization modules in association with said access device, wherein at least one of said plurality of authorization modules receives fingerprint data from a user in order to authorize said user to utilize said access device, wherein said fingerprint data is processed by said at least one of said plurality of authorization modules and wherein at least one other of said plurality of authorization modules receives an authorization code from a memory location.

The Applicant further notes that independent claim 46 has also been amended as follows:

> An access control method, comprising:
> providing an access device;
> providing at least two types of authorization devices wherein said at least two types of authorization devices transmit data to said access device;
> associating a plurality of authorization modules with said access device; and

authorizing a user to utilize said access device based said data received by said at least one of said plurality of authorization modules.

Applicant's claim limitations relate to a plurality of authorization modules wherein one module receives fingerprint data (fingerprint keyfob) and one module receives and an authorization code form a memory location (badge). In other words, the access control system is capable of receiving data from both a badge and a fingerprint keyfob. The access system utilizes a plurality of software modules to determine if the authorization code is from a badge or a keyfob and then process the received data. This is disclosed in paragraph [0027] as follows:

> [0027] As can be seen, the reader 12 of the security system 10 as described above *is capable of performing the functions of both a badge reader and a keyfob receiver such that the reader 12 uses the same RF protocol in interacting with the badge 20 and the keyfob 24.* Accordingly, the reader 12 is a dual-technology reader that is able to provide a simple low-cost badging technology and a higher security level solution that provides significantly higher authentication reliability using the same door reader hardware. Consequently, a supplier of access security systems can maintain a smaller inventory that includes badges, keyfobs, and only one type of reader. Moreover, a user can easily increase the level of security by simply substituting or adding keyfobs to its security system. (emphasis added)

This is also disclosed in the Applicant's paragraphs [0025] - [0026] as shown above and in FIG. 4.

Fitzgibbon does not disclose this limitation of a plurality of *authorization modules* in an access system which can receive data from two different types of access devices. The Examiner has cited the abstract of U.S. Patent No. 5,949,349 (issued to Farris et al.) and incorporated by reference by Fitzgibbon, for the plurality of authorization modules; however, Farris does not disclose a *plurality* of authorization modules. Farris discloses an access system which can receive rolling codes and non-rolling codes without specifically disclosing a plurality of authorization *modules*. Fitzgibbon/Farris also does not disclose a *plurality* of authorization modules wherein one module receives fingerprint data and one module receives an authorization code form a memory location (i.e. a badge).

The Applicant also notes that dependent claims 39 and 47 have been amended to the processor "comprising" the authorization modules, and to include the access to area or a "controlled apparatus or process" utilizing said access device.

Fitzgibbon, as shown above, does not disclose each and every limitation of the Applicant's independent claims 38 and 45 and therefore fails in the aforementioned *prima facie* anticipation test. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §102(e) rejections of claims 38-41, 45-49 and 53 based on the Fitzgibbon reference be withdrawn.

III. Claim Rejections - 35 USC § 103

Requirements for Prima Facie Obviousness

The obligation of the examiner to go forward and produce reasoning and evidence in support of obviousness is clearly defined at M.P.E.P. §2142:

> "The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness."

The U.S. Supreme Court ruling of April 30, 2007 (*KSR Int'l v. Teleflex Inc.*) states:

"The TSM test captures a helpful insight: A patent composed of several elements is not proved obvious merely by demonstrating that each element was, independently, known in the prior art. Although common sense directs caution as to a patent application claiming as innovation the combination of two known devices according to their established functions, it can be important to identify a reason that would have prompted a person of ordinary skill in the art to combine the elements as the new invention does."

"To facilitate review, this analysis should be made explicit."

The U.S. Supreme Court ruling states that it is important to identify a *reason* that would have prompted a person to combine the elements and to make that analysis *explicit*. MPEP §2143 sets out the further basic criteria to establish a *prima facie* case of obviousness:

1. a reasonable expectation of success; and

2. the teaching or suggestion of all the claim limitations by the prior art reference (or references when combined).

It follows that in the absence of such a *prima facie* showing of obviousness by the Examiner (assuming there are no objections or other grounds for rejection) and of a *prima facie* showing by the Examiner of a *reason* to combine the references, an applicant is entitled to grant of a patent. Thus, in order to support an obviousness rejection, the Examiner is obliged to produce evidence compelling a conclusion that the basic criterion has been met.

Berardi in view of Fitzgibbon

The Examiner rejected claims 1-7, 9-16, 18-21, and 23-25 under 35 U.S.C. §103(a) as being unpatentable over Berardi in view of Fitzgibbon.

The Examiner argued that Berardi shows a method for providing access to a financial transaction, where the system includes two versions of the transponder 102. The Examiner stated that the first embodiment of transponder 102 does not include a fingerprint reader (citing FIG. 2); the Examiner has interpreted this as a badge. The Examiner stated that the second embodiment of transponder 102 includes a fingerprint reader (FIG. 9); the Examiner has interpreted this as a keyfob. The Examiner stated that the FIG. 9 transponder sends the fob ID (citing stored in memory 214) with the fingerprint so both can be authenticated. The Examiner stated that when the data is read from the transponder, a comparison is made to authorize financial access; the Examiner argued that this meets the limitation of determining if the received code is authentic and providing access upon authentication.

The Examiner stated that if the data is from a badge, the authorization step compares account data (or the transponder ID) (citing paragraph [0059]); if the data is from a keyfob the authorization step compares fingerprint data (citing paragraph [0141]). It is the Examiner's position that in order to compare the received data from the FIG. 9 transponder with stored fingerprint data, a decision inherently is made that the data received includes fingerprint data. The Examiner argued that this meets the limitation of determining if the code is from a badge or a keyfob.

The Examiner argued that in an analogous art, Fitzgibbon teaches an access security system where a transmitter can send codes to a garage door for an access authorization. The Examiner stated that the portable transmitter (authorization module) can additionally include a fingerprint reader to send information regarding the user's fingerprint, also for authorization. The Examiner argued that Fitzgibbon includes a processor (citing FIG. 4) in communication with the transmitters to process data received and make an authorization determination (citing FIG. 8). The Examiner cited Fitzgibbon for teaching that in this type of system, the use of rolling codes can improve the security of the system. The Examiner stated that the fingerprints and rolling codes are separately checked against databases for authenticity (citing FIG. 8).

The Examiner argued that, therefore, it would have been obvious to one of ordinary skill in t he art at the time of the invention to have used the fingerprint and rolling code processing of Fitzgibbon in the fingerprint entry transponder embodiment of Berardi because adding rolling code authentication increases security in the system.

The Applicant respectfully disagrees with this assessment and notes that the arguments presented above against the §102 rejections over Berardi and Fitzgibbon apply equally against the §103 rejections over Berardi in view of Fitzgibbon, as neither Berardi nor Fitzgibbon disclose each and every limitation of

the Applicant's claims. The Applicant further notes that independent claims 1, 7 and 14 have been amended to clarify the distinction between a badge and a keyfob and therefore to clarify that the reader is capable of receiving data from both a badge and a keyfob. As argued above, neither Berardi nor Fitzgibbon disclose a reader that is a capable of receiving data from both a badge and a keyfob.

The Applicant also submits that Fitzgibbon is not in an analogous art as it is not relevant to the *particular problem* with which the Applicant is involved. The Applicant notes that MPEP §2141.01(a) states: "*State Contracting & Eng'g Corp. v. Condotte America, Inc.*, 346 F.3d 1057, 1069, 68 USPQ2d 1481, 1490 (Fed. Cir. 2003) (where the general scope of a reference is outside the pertinent field of endeavor, the reference may be considered analogous art if subject matter disclosed therein is relevant to the particular problem with which the inventor is involved)".

The particular problem with which the Applicant is involved is solving the problem of different reader systems which are presently incompatible with each other and with users requiring different levels of security. This is disclosed in paragraph [0005] as follows:

> "Different users require different levels of security. Thus, the security requirements of some users may be satisfied with badges and a badge reader as described above, while other users may require the higher level of security provided by the keyfob described above. In order to fill both requirements, a supplier of access security systems is obliged to maintain an inventory that includes badges, badge receivers, keyfobs, and keyfob receivers."

Fitzgibbon is not relevant to this particular problem, and therefore not analogous art, but is relevant to the security of a garage door.

Amended claim 1 is shown as follows, with emphasis added:

> A security system reader comprising:
> a transceiver that transmits a *single* stimulus signal to *both a badge and a fingerprint keyfob* and that *receives a signal containing an authentication code transmitted from either the badge or the fingerprint keyfob*; and,

> a *processor that determines whether the received authentication code is from the badge or the fingerprint keyfob*, and that performs an authentication of the authentication code dependent upon whether the authentication code is from the badge or from the fingerprint keyfob, *wherein the authentication code from the badge is retrieved from a memory location contained within the badge* and wherein the processor matches the authentication code from the badge to a list of authorized authorization codes and *wherein the authentication code from the fingerprint keyfob comprises a digitized fingerprint signature and a rolling identifier,* and wherein the processor is arranged to perform an authentication of the authentication code based upon both the digitized fingerprint signature and the rolling identifier in the authentication code from the fingerprint keyfob.

Independent claims 7 and 14 are similar to claim 1 in that all three claims include the limitation of receiving signals from either a badge or a keyfob, wherein a badge receive the authorization code form a memory location and the keyfob digitalizes a fingerprint with a rolling code. Neither Berardi nor Fitzgibbon, singularly or in combination, disclose that the reader and processor are capable of receiving and transmitting signals to <u>both</u> a badge and a fingerprint keyfob. This limitation is disclosed in the Applicant's paragraphs [0025] - [0026] as shown above and in paragraph [0027] as follows:

> [0027] As can be seen, the reader 12 of the security system 10 as described above is *capable of performing the functions of <u>both</u> a badge reader and a keyfob receiver* such that the reader 12 uses the same RF protocol in interacting with the badge 20 and the keyfob 24. Accordingly, *the reader 12 is a dual-technology reader* that is able to provide a simple low-cost badging technology and a higher security level solution that provides significantly higher authentication reliability using the same door reader hardware. Consequently, a supplier of access security systems can maintain a smaller inventory that includes badges, keyfobs, and only one type of reader. Moreover, a user can easily increase the level of security by simply substituting or adding keyfobs to its security system. (emphasis added)

As neither Berardi nor Fitzgibbon discloses this limitation, the combination of Berardi and Fitzgibbon fails in the aforementioned *prima facie* obviousness test as <u>each</u> and <u>every</u> limitation of the Applicant's claims 1, 7 and 14 are not disclosed. Claims dependent upon these independent claims are, therefore, also not disclosed in Berardi in view of Fitzgibbon. Based on the foregoing, the Applicant respectfully

requests that the 35 U.S.C. §103(a) rejections of claims 1-7, 9-16, 18-21, and 23-25 based on Berardi in view of Fitzgibbon be with drawn.

The Examiner rejected claims 35-37 under 35 U.S.C. 103(a) as being unpatentable over Berardi as applied to claim 32 above, and further in view of Fitzgibbon.

The Examiner argued that in an analogous art, Fitzgibbon teaches an access security system where a transmitter can send codes to a garage door for access authorization. The Examiner stated that the portable transmitter (authorization module) can additionally include a fingerprint reader to send information regarding the user's fingerprint, also for authorization. The Examiner argued that Fitzgibbo9n includes a processor (citing FIG. 4) in communication with the transmitters to process data received and make an authorization determination, (citing FIG. 8).

The Examiner argued that, therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have used the fingerprint and rolling code processing of Fitzgibbon in the fingerprint entry transponder embodiment of Berardi because adding rolling code authentication increases security in the system.

The Applicant respectfully disagrees with this assessment and notes that the arguments presented above against the §102 rejection of claim 32 over Berardi applies equally against the §103 rejections of claims 35-36 as these claims are dependent upon independent claim 32. The Applicant further notes that claim 37 has been cancelled, rendering moot the Examiner's argument against this claim.

As argued above, Berardi does not disclose an access system which is capable of receiving signals from both a badge and a keyfob and thereafter processing these authentication signals in different manners, as claimed in independent claim 32. This is also not disclosed in the Fitzgibbon reference and therefore, Berardi in view of Fitzgibbon fails in the aforementioned *prima facie*

obviousness test as each and every limitation of the Applicant's claims 35-36 is not disclosed.

Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §103(a) rejections of claims 35-36 based on Berardi in view of Fitzgibbon be withdrawn.

Fitzgibbon in view of Berardi

The Examiner rejected claims 42-44 and 50-52 under 35 U.S.C. 103(a) as being unpatentable over Fitzgibbon as applied to claims 38 and 46 above, further in view of Berardi.

The Examiner argued that Berardi shows an access control system including a transponder, which may be embodied in a fob, tag, card (citing paragraph 21). The Examiner argued that the FIG. 9 transponder sends the fob ID (citing stored in memory 214) with the fingerprint so both can be authenticated, thereby suggesting a fingerprint fob.

The Examiner argued that, therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have formed the Fitzgibbon controller into a key fob or a card since Berardi suggests these embodiments for an access device and such physical embodiments are recognized in the art as easily portable.

The Applicant respectfully disagrees with this assessment and notes that the arguments presented above against the §102 rejections of claims 38 and 46 apply equally against the §103 rejections of dependent claims 42-44 and 50-52. Neither Fitzgibbon nor Berardi disclose of a *plurality* of authorization modules in an access system which can receive data from *two* different types of access devices.

The Applicant further notes that claim 42-43 and 50-51 have been amended to clarify that the plurality of authorization modules comprises a keyfob reader and claims 44 and 52 have been amended to amend "card" reader to "magnetic stripe"

reader. The keyfob reader is disclosed, as above, in paragraphs [0025] - [0027] and the magnetic stripe reader is disclosed in paragraph [0017].

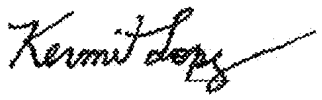
The combination of Fitzgibbon and Berardi fails in the aforementioned *prima facie* obviousness test as neither Fitzgibbon nor Berardi disclose each and every limitation of the Applicant's independent claims 38 and 46, as shown above. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §103(a) rejections of claims 42-44 and 50-52 based on Fitzgibbon in view of Berardi be withdrawn.

V. Conclusion

In view of the foregoing discussion, the Applicant has responded to each and every rejection of the Official Action. The Applicant has clarified the structural distinctions of the present invention. Applicant respectfully requests the withdrawal of the rejections under 35 U.S.C. §102 and 35 U.S.C. §103 based on the preceding remarks. Reconsideration and allowance of Applicant's application is also respectfully solicited.

Should there be any outstanding matters that need to be resolved, the Examiner is respectfully requested to contact the undersigned representative to conduct an interview in an effort to expedite prosecution in connection with the present application.

Respectfully submitted,



Dated: July 13, 2007

Kermit Lopez
Attorney for Applicants
Registration No. 41,953
ORTIZ & LOPEZ, PLLC
P.O. Box 4484
Albuquerque, NM 87196-4484